UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,898	08/01/2003	Philip Kwan	FOUND-0057 (434103-048)	9803

49680 7590 02/18/2010

FOUNDRY-NIXON PEABODY LLP
P.O. Box 60610
Palo Alto, CA 94306

EXAMINER	
CHAN, SAI MING	
ART UNIT	**PAPER NUMBER**
2462	
MAIL DATE	**DELIVERY MODE**
02/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/631,898	KWAN, PHILIP	
	Examiner	Art Unit	
	SAI-MING CHAN	2462	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-12,15-21,24-29,31-39 and 41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-12,15-21,24-29,31-39 and 41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statements (IDS) submitted on 1/29/2010 has been considered by the Examiner and made of record in the application file.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-2, 5-12, 15-21, 24-29, 31-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Meier et al. (U.S. Patent Publication # 20050185626)**, in view of **Palekar et al. (U.S. Patent Publication #20030226017),** and in view of **Kalavade et al. (U.S. Patent Publication #20030051041)**.

Consider **claim 1,** Meier et al. clearly disclose and show a computer implemented method comprising:

at a network access device (fig. 3 (102)) communicably coupled to a host network (paragraph 0004 (network)), sensing a user device (fig. 3 (302), paragraph 0032 (WSTA attempting to gain access to AP)) coupled to a port of a network access device (paragraph 0032 (attempting to gain access to AP)); and

placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show determining if the user device supports a user authentication protocol used by the host network (para. 0049 (if user supports authentication protocol)), the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity));

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 0169 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access

device and placing semi-authorized access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.

Consider **claims 11 and 36,** Meier et al. clearly disclose and show a network access device comprising:

a plurality of input ports (para. 0003 (access point; Examiner notes that AP has plurality of input ports));

a plurality of output ports (para. 0003 (access point; Examiner notes that AP has plurality of output ports));

a switching fabric for routing data received on the plurality of input ports to at least one of the plurality of output ports (para. 0003 (access point)); and

placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show control logic adapted to determine whether a user device coupled to one of the plurality of input ports supports a user authentication protocol used by a host network (para. 0049 (if user supports authentication protocol)), and the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user

authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 0169 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access device and placing semi-authorized access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.

Claim 20. (Currently Amended) A network system, comprising:

a host network (paragraph 0004 (network)) that uses a user authentication protocol (para. 0003 (RADIUS));

a network access device (fig. 3 (302), paragraph 0032 (WSTA attempting to gain access to AP)) communicatively coupled to the host network (paragraph 0032 (attempting to gain access to AP)); and

a user device (fig. 3 (302), paragraph 0032 (WSTA)) coupled to a port of the network access device (para. 0003 (assign a station));

placing the port in a semi-authorized access state, the semi-authorized access state providing the user device with limited network access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show control logic adapted to determine whether a user device coupled to one of the plurality of input ports supports a user authentication protocol used by a host network (para. 0049 (if user supports authentication protocol)), and the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier,

and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 0169 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access device and placing semi-authorized access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.

Consider **claim 31,** Meier et al. clearly disclose and show an apparatus comprising:

means (paragraph 0010 (means)) for sensing a user device (fig. 3 (302), paragraph 0032 (AP receives a message from WSTA that it attempts to gain access to

AP)) coupled to a port of a network access device (paragraph 0032 (attempting to gain access to AP)); and

means (paragraph 0010 (means)) for placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) if it is determined that the user device does not support the user authentication protocol (paragraph 0022 (unauthorized guest WSTAs)), the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show means for determining if the user device supports a user authentication protocol used by the host network (para. 0049 (if user supports authentication protocol)), the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity));

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 0169 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access device and placing semi-authorized access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.

Consider **claims 32** and **41,** Meier et al. clearly disclose a computer implemented method comprising:

at a network access device (fig. 3 (102)) communicably coupled to a host network (paragraph 0004 (network)), sensing a user device (fig. 3 (302), paragraph 0032 (WSTA attempting to gain access to AP)) coupled to a port of a network access device (paragraph 0032 (attempting to gain access to AP)); and

placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show determining if the user device supports a user authentication protocol used by the host network (para. 0049 (if user supports authentication protocol)), the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity));

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 0169 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier,

show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access device and placing semi-authorized access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.

Consider **claim 2,** and as applied to **claim 1** above,

claim 12, and as applied to **claim 11** above,

claim 21, and as applied to **claim 20** above,

Meier et al., clearly disclose and show a method, wherein said pre-configured network comprises a Voice over Internet Protocol (VoIP) network (paragraph 0003 (Voice over IP)).

Consider **claim 5,** and as applied to **claim 1** above,

claim 15, and as applied to **claim 11** above,

claim 24, and as applied to **claim 20** above,

Meier et al., clearly disclose and show a method, wherein the placing comprises selectively placing said port into one of a plurality of semi-authorized access states (paragraph 0022 (default guest set)).

Consider **claim 6**, and as applied to **claim 5** above,

claim 16, and as applied to **claim 15** above,

claim 25, and as applied to **claim 24** above,

Meier et al., clearly disclose and show a method, wherein the placing comprises:

determining a type of the user device (paragraph 0008 (type of service for the wireless station)) ; and

selectively placing said port into one of a plurality of semi-authorized access states (paragraph 0022 (default guest set)) based on the type of user device (paragraph 0009 (identifies a type of service for the station).

Consider **claim 7,** and as applied to **claim 6** above,

claim 17, and as applied to **claim 16** above,

claim 26, and as applied to **claim 25** above,

Meier et al., clearly disclose and show a method, wherein selectively placing comprises selectively placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) that limits access by the user device to a network (paragraph 0022 (restricted access)) comprising a Voice over Internet Protocol network (paragraph 0003 (Voice over IP)).

Consider **claim 8,** and as applied to **claim 6** above,

claim 18, and as applied to **claim 16** above,

claim 27, and as applied to **claim 25** above,

Meier et al., clearly disclose and show a method, wherein selectively placing comprises selectively placing the port into a semi-authorized access state (paragraph 0022 (default

guest set)) that limits access by said user device (paragraph 0022 (restricted access)) to a network comprising the Internet (abstract (IP)) if said user device is a portable computing device (fig. 2 (208)).

Consider **claim 9,** and as applied to **claim 1** above,

claim 19, and as applied to **claim 11** above,

claim 28, and as applied to **claim 20** above,

Meier et al., clearly disclose and show a method, wherein said user authentication protocol is IEEE 802.1x (paragraph 0029 (802.11)).

Consider **claim 10**, and as applied to **claim 1** above,

claim 29, and as applied to **claim 20** above,

Meier et al., clearly disclose and show a method, wherein said network access device comprises a network switch (paragraph 95, lines 1-8 (network switches)).

Consider **claim 33,** and as applied to **claim 32** above,

claim 37, and as applied to **claim 36** above

Meier et al. clearly disclose and show performing further user authentication in accordance with the user authentication protocol if it is determined that the user device is able to communicate using the user authentication protocol (paragraph 0021 (pass any authentication criteria defined for its SSID)).

Consider **claim 34,** and as applied to **claim 32** above, i

claim 38, and as applied to **claim 36** above,

wherein the limited access comprises less access than access afforded a user device that is successfully authenticated using the user authentication protocol (para. 0019 (differentiate for security purposes)).

Consider **claim 35,** and as applied to **claims 34** above,

claim 39, and as applied to **claim 36** above,

wherein the limited access comprises access to a low-security Virtual Local Area Network (VLAN) (para. 0019 (differentiate for security purposes)).

Response to Arguments

Applicant's arguments filed on 8/28/2009, with respect to claims 1, 11, 20, 30-32 and 40-41, on pages 2-16 of the remarks, have been carefully considered.

In the present application, Applicants basically argues that Meier et al. does not teach or suggest "determining, by the network access device, if the user device supports a user authentication protocol used by the host" and ""placing, by the network access device, the port in a semi-authorized access state". The Examiner has modified the response with a new reference which provides "determining, by the network access device, if the user device supports a user authentication protocol used by the host" and

“”placing, by the network access device, the port in a semi-authorized access state”. See the above rejections of claims 1, 11, 20, 30-32 and 40-41, for the relevant interpretation and citations found in Kalavade, disclosing the new limitations.

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Sai-Ming Chan whose telephone number is (571) 270-1769. The Examiner can normally be reached on Monday-Thursday from 6:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner’s supervisor, Seema Rao can be reached on (571) 272-3174. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

/Sai-Ming Chan/

Examiner, Art Unit 2462

February 4, 2010

/Donald L Mills/
Primary Examiner, Art Unit 2462